United Nations A/HRC/39/29

General Assembly

Distr.: General
3 August 2018

Original: English

Human Rights Council
Thirty-ninth session
Agenda items 2 and 3
Annual report of the United Nations High Commissioner for Human Rights and reports of the Office of the High Commissioner and the Secretary-General

Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

The right to privacy in the digital age

Report of the United Nations High Commissioner for Human Rights

Summary

The present report is submitted pursuant to resolution 34/7, in which the Human Rights Council requested the High Commissioner for Human Rights to prepare a report identifying and clarifying principles, standards and best practices regarding the promotion and protection of the right to privacy in the digital age, including the responsibility of business enterprises in this regard, and present it to the Human Rights Council at its thirty-ninth session.

GE.18-12799(E)
1812799

Please recycle

I. Introduction

1. The need to address the challenges that the digital world brings to the right to privacy is more acute than ever. Driven mostly by the private sector, digital technologies that continually exploit data linked to people's lives, are progressively penetrating the social, cultural, economic and political fabric of modern societies. Increasingly powerful data-intensive technologies, such as big data and artificial intelligence, threaten to create an intrusive digital environment in which both States and business enterprises are able to conduct surveillance, analyse, predict and even manipulate people's behaviour to an unprecedented degree. While there is no denying that data-driven technologies can be put to highly beneficial uses, these technological developments carry very significant risks for human dignity, autonomy and privacy and the exercise of human rights in general if not managed with great care.

2. International and regional actors are increasingly aware of the challenges and beginning to act accordingly. The Human Rights Council mandated a Special Rapporteur on the right to privacy in July 2015. In numerous resolutions, the Human Rights Council and the General Assembly have expressed concerns about the risks to privacy emanating from State surveillance measures and business practices.[1] At the regional level, several measures have strengthened data privacy protections, such as the European Union General Data Protection Regulation, which has recently taken effect with global implications; the Council of Europe protocol to update and modernize the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the African Union Commission Personal Data Protection Guidelines for Africa. At the same time, many Governments have adopted laws or proposed legislation that increases their surveillance powers, often in ways that fall short of applicable international human rights standards.[2]

3. The present report provides guidance on how to address some of the pressing challenges that the right to privacy faces in the digital age. It provides a brief overview of the international legal framework and includes a discussion of the most significant current trends. It then turns to the obligations of States and the responsibility of business enterprises, including a discussion of adequate safeguards and oversight. The final chapter gives some insights into how remedies can be provided for privacy infringements and abuses.

4. The report builds on the 2014 report by the High Commissioner on the right to privacy in the digital age (A/HRC/27/37) and on the presentations and discussions at an expert workshop that took place in Geneva in February 2018.[3] It also relies on 63 written submissions received from a wide range of stakeholders.[4]

II. Understanding the right to privacy in the digital age

5. The right to privacy is a fundamental human right, recognized in article 12 of the Universal Declaration of Human Rights, article 17 of the International Covenant on Civil and Political Rights and in many other international and regional human rights

[1] See, for example, General Assembly resolutions 68/167, 69/166 and 71/199 and Human Rights Council resolutions 28/16 and 34/7 and decision 25/117.

[2] See, for example, Anja Seibert-Fohr, "Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy" (April 2018), available from https://ssrn.com/abstract=3168711; https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee and www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyin DigitalAge/SR_right_privacy.pdf.

[3] See www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgePrivacyWorkhop.aspx and webcast available at http://webtv.un.org/search/part-1.1-un-expert-workshop-on-the-right-to-privacy-in-the-digital-age/5734527899001/?term=2018-02-19&sort=date&page=2.

[4] All submissions are available at www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

instruments.[5], [6] Privacy can be considered as the presumption that individuals should have an area of autonomous development, interaction and liberty, a "private sphere" with or without interaction with others, free from State intervention and from excessive unsolicited intervention by other uninvited individuals (see, for example, A/HRC/13/37, para. 11, and A/HRC/23/40, paras. 22 and 42). In the digital environment, informational privacy, covering information that exists or can be derived about a person and her or his life and the decisions based on that information, is of particular importance.

6. The protection of the right to privacy is broad, extending not only to the substantive information contained in communications but equally to metadata as, when analysed and aggregated, such data "may give an insight into an individual's behaviour, social relationship, private preference and identity that go beyond even that conveyed by accessing the content of a communication" (see A/HRC/27/37, para. 19). The protection of the right to privacy is not limited to private, secluded spaces, such as the home of a person, but extends to public spaces and information that is publicly available (see CCPR/C/COL/CO/7, para. 32). For example, the right to privacy comes into play when a Government is monitoring a public space, such as a marketplace or a train station, thereby observing individuals. Similarly, when information that is publicly available about an individual on social media is collected and analysed, it also implicates the right to privacy.[7] The public sharing of information does not render its substance unprotected.[8]

7. The right to privacy is not only impacted by the examination or use of information about a person by a human or an algorithm.[9] Even the mere generation and collection of data relating to a person's identity, family or life already affects the right to privacy, as through those steps an individual loses some control over information that could put his or her privacy at risk (see A/HRC/27/37, para. 20).[10] In addition, the mere existence of secret surveillance amounts to an interference with the right to privacy (ibid).[11]

8. The right to privacy applies equally to everyone. Any differences in its protection on the basis of nationality or any other grounds are inconsistent with the right to equality and non-discrimination contained in article 26 of the International Covenant on Civil and Political Rights.

9. A State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State party, even if not situated within its territory.[12] Human rights law applies where a State exercises its power or effective control in relation to digital communications infrastructure, wherever located, for example through direct tapping or penetration of communications infrastructure located outside the territory of that State. Equally, where a State exercises regulatory jurisdiction over a third party that controls a person's information (for example, a cloud service provider), that State also has to extend human rights protections to those whose privacy would be affected by accessing or using that information (see A/HRC/27/37, para. 34).

---

[5] See, for example, article 16 of the Convention on the Rights of the Child; article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families; and article 22 of the Convention on the Rights of Persons with Disabilities.

[6] See, for example, article 10 of the African Charter on the Rights and Welfare of the Child; article 11 of the American Convention on Human Rights; and article 8 of the European Convention on Human Rights.

[7] See Privacy International submission for the present report.

[8] Anja Seibert-Fohr, "Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy".

[9] See Paul Bernal, "Data gathering, surveillance and human rights: recasting the debate", *Journal of Cyber Policy*, vol. 1, No. 2 (2016).

[10] See also European Court of Human Rights, *Rotaru v. Romania*, application No. 28341/95, judgment of 4 May 2000 and *Kopp v. Switzerland*, application No. 23224/94, judgment of 25 March 1998.

[11] See also European Court of Human Rights, *Roman Zakharov v. Russia*, application No. 47143/06, judgment of 4 December 2015.

[12] See Human Rights Committee, general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant, para. 10.

19. According to article 17 of the Covenant, any interference is only permissible if it is neither arbitrary nor unlawful. Human rights mechanisms have consistently interpreted those words as pointing to the overarching principles of legality, necessity and proportionality (see A/HRC/27/37, paras. 21–27).[13] In keeping with those principles, States may only interfere with the right to privacy to the extent envisaged by the law and the relevant legislation must specify in detail the precise circumstances in which such interference may be permitted.[14] Interference is unlawful and arbitrary not only when it is not provided for by law but also when a law or the particular interference is in conflict with the provisions, aims and objectives of the Covenant.[15] A limitation can only be lawful and non-arbitrary if it serves a legitimate purpose (see A/HRC/29/32, para. 33). The limitation must be necessary for reaching that legitimate aim and in proportion to that aim and must be the least intrusive option available. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless (see A/69/397, para. 51).

11. The right to privacy is central to the enjoyment and exercise of human rights online and offline. It serves as one of the foundations of a democratic society and plays a key role for the realization of a broad spectrum of human rights, ranging from freedom of expression (see A/HRC/23/40 and A/HRC/29/32, para. 15) and freedom of association and assembly (see A/HRC/31/66, paras. 73–78 and A/72/135, paras. 47–50) to the prohibition of discrimination and more.[16] Interference with the right to privacy can have a disproportionate impact on certain individuals and/or groups, thus exacerbating inequality and discrimination.[17] Overbroad privacy regulations may also amount to undue limitations of other rights, in particular freedom of expression, for example when a disproportionate regulation interferes with legitimate news reporting, artistic expression or scientific research. For lack of space, the interrelationship between the right to privacy and all other human rights, its discriminatory impact on specific individuals and groups, and approaches to protect them cannot be examined in the present report.

III. Privacy interferences: trends and concerns

A. Increased reliance on personal data by Governments and business enterprises

Growing digital footprints

12. Both States and business enterprises collect and use steadily increasing amounts of data related to the private lives of individuals. Immense data streams relating to billions of individuals are being collected by personal computers, smartphones, smartwatches, fitness trackers and other wearables. A rapidly growing number of other interconnected devices and sensors installed in so-called smart homes and smart cities add further data. The range and depth of the information collected and used are vast, from device identifiers, email addresses and phone numbers to biometric, health and financial data and behavioural patterns. Much of this happens without the knowledge of the persons concerned and without meaningful consent.

Data sharing and fusion

13. Business enterprises and States continuously exchange and fuse personal data from various sources and databases, with data brokers assuming a key position. As a consequence, individuals find themselves in a position of powerlessness, as it seems almost

[13] See also Human Rights Council resolution 34/7, para. 2.

[14] See Human Rights Committee, general comment No. 16 (1988) on the right to privacy, paras. 3 and 8.

[15] Ibid., para. 4.

[16] See Paul Bernal, "Data gathering, surveillance and human rights: recasting the debate".

[17] See General Assembly resolution 71/199, para. 5 (g); Human Rights Council resolution 34/7, para. 5 (g); and International Network of Civil Liberties Organizations, submission for the present report.

impossible to keep track of who holds what kind of information about them, let alone to control the many ways in which that information can be used.

Biometric data

14. States and business enterprises increasingly deploy systems relying on the collection and use of biometric data, such as DNA, facial geometry, voice, retina or iris patterns and fingerprints. Some countries have created immense centralized databases storing such information for a diverse range of purposes, from national security and criminal investigation to the identification of individuals for purposes of the provision of essential services, such as social and financial services and education. State actors around the world deploy closed-circuit television cameras in cities, train stations or airports that use facial recognition to automatically identify and flag persons. Biometric-based technologies are increasingly used to control migration, both at borders and within countries. The creation of mass databases of biometric data raises significant human rights concerns. Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is worrisome that some States are embarking on vast biometric data-based projects without having adequate legal and procedural safeguards in place.

Growing analytical power

15. The analytical power of data-driven technology continues to grow exponentially. Big data analytics and artificial intelligence increasingly enable States and business enterprises to obtain fine-grained information about people's lives, make inferences about their physical and mental characteristics and create detailed personality profiles. Many systems used by Governments and business enterprises are built for that precise purpose — maximizing the amount of information on individuals in order to analyse, profile, assess, categorize and eventually make decisions, often automated, about them.

16. The resulting environment carries risks for individuals and societies that can hardly be overestimated. For example, recent years have seen data breaches of huge scope, exposing the persons concerned to identity theft and the disclosure of intimate information. Illegitimate data collection and analysis have been connected to the targeting of voters. Profiles, "scoring" and "ranking" of individuals can be used for assessing eligibility for health care, other insurance coverage, financial services and beyond. Opaque data-based decisions in high-stakes cases, for example in sentencing procedures and recidivism assessments, may threaten due process. Attempts to identify individuals as potential security threats in the context of predictive policing raise concerns, given the issues surrounding transparency, overbreadth, accountability and the potential for discriminatory outcomes.[18]

B. State surveillance and communications interception

Mass surveillance

17. Many States continue to engage in secret mass surveillance and communications interception, collecting, storing and analysing the data of all users relating to a broad range of means of communication (for example, emails, telephone and video calls, text messages and websites visited). While some States claim that such indiscriminate mass surveillance is necessary to protect national security, this practice is "not permissible under international human rights law, as an individualized necessity and proportionality analysis would not be

[18] See Ajay Sandhu, "Data driven policing: highlighting some risks associated with predicting crime", Human Rights Centre, Essex University

possible in the context of such measures" (see A/HRC/33/29, para. 58).[19] As the European Court of Human Rights has pointed out, "a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it".[20]

Access to the user data of business enterprises

18. States often rely on business enterprises for the collection and interception of personal data. For example, some States compel telecommunications and Internet service providers to give them direct access to the data streams running through their networks. Such systems of direct access are of serious concern, as they are particularly prone to abuse and tend to circumvent key procedural safeguards.[21] Some States also demand access to the massive amounts of information collected and stored by telecommunications and Internet service providers. States continue to impose mandatory obligations on telecommunications companies and Internet service providers to retain communications data for extended periods of time.[22] Many such laws require the companies to collect and store indiscriminately all traffic data of all subscribers and users relating to all means of electronic communication. They limit people's ability to communicate anonymously, create the risk of abuses and may facilitate disclosure to third parties, including criminals, political opponents, or business competitors through hacking or other data breaches. Such laws exceed the limits of what can be considered necessary and proportionate.[23]

Hacking

19. Governments appear to rely increasingly on offensive intrusion software that infiltrates individuals' digital devices. This type of hacking enables indiscriminate interception and collection of all kinds of communications and data, encrypted or not, and also permits remote and secret access to personal devices and data stored on them, enabling the conduct of real-time surveillance and manipulation of data on such devices.[24] That poses risks not only for the right to privacy but also for procedural fairness rights when such evidence may be used in legal proceedings (see A/HRC/23/40, para. 62). Hacking also raises significant extraterritoriality concerns, as it can affect individuals across many jurisdictions.[25] Furthermore, hacking relies on exploiting vulnerabilities in information and communications technology (ICT) systems and thus contributes to security threats for millions of users.

Attempts at weakening encryption and anonymity

20. Recurring attempts by States to weaken encryption technology and limit access to anonymity tools similarly threaten the security and confidentiality of communications and other activities online. Some States call for mandated back doors in encrypted communications, require providers of encrypted communications services to hand over encryption keys (see A/HRC/29/32, paras. 38–45) or even ban or block certain secure communications applications, including encrypted messaging and virtual private and anonymization networks. Encryption and anonymity provide individuals and groups with a zone of privacy online where they can hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks (A/HRC/29/32).[26] Encryption and

[19] See also A/HRC/27/37, para. 25.

[20] See *Roman Zakharov v. Russia*, para. 232.

[21] See *Roman Zakharov v. Russia*, para. 270.

[22] See CCPR/C/ZAF/CO/1, paras. 42–43, and CCPR/C/PAK/CO/1, paras. 35–36.

[23] See, for example, European Court of Justice joined cases C-203/15 and C-698/15, *Tele2 Sverige AB v. Swedish Post and Telecom Authority and Secretary of State for the Home Department v. Watson*, judgment of 21 December 2016, para. 107; CCPR/C/ZAF/CO/1, paras. 42–43; and CCPR/C/CMR/CO/5, paras. 39–40.

[24] See Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "Encryption and anonymity follow-up report" (June 2018).

[25] See submission of Privacy International.

[26] See also UCI Law International Justice Clinic, "Selected references: unofficial companion to report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and the freedom of expression";

anonymity tools are widely used around the world, including by human rights defenders, civil society, journalists, whistle-blowers and political dissidents facing persecution and harassment. Weakening them jeopardizes the privacy of all users and exposes them to unlawful interferences not only by States, but also by non-State actors, including criminal networks.[27] Such a widespread and indiscriminate impact is not compatible with the principle of proportionality (see A/HRC/29/32, para. 36).

Intelligence-sharing

21. Governments across the globe routinely share intelligence on individuals outside any legal framework and without adequate oversight.[28] Intelligence-sharing poses the serious risk that a State may use this approach to circumvent domestic legal constraints by relying on others to obtain and then share information. Such a practice would fail the test of lawfulness and may undermine the essence of the right to privacy (see A/HRC/27/37, para. 30). The threat to human rights protections is particularly acute where intelligence is shared with States with weak rule of law and/or a history of systematically violating human rights. Intelligence received by one State from another may have been obtained in violation of international law, including through torture and other cruel, inhuman or degrading treatment. The human rights risks posed by intelligence-sharing are heightened by the current lack of transparency, accountability and oversight of intelligence-sharing arrangements (see A/69/397, para. 44, CCPR/C/GBR/CO/7, para. 24, and CCPR/C/SWE/CO/7, para. 36). With very few exceptions, legislation has failed to place intelligence-sharing on a proper statutory footing, compliant with the principle of legality under international human rights law.[29]

Cross-border access to data held by business enterprises

22. Recently, there have been efforts to create legal mechanisms aimed at facilitating the access of States to personal information stored on the servers of business enterprises abroad. Obtaining evidence in the course of a criminal investigation is without doubt an important and legitimate goal. However, such access can result in weakening or circumventing procedural safeguards, such as the requirement for authorization by an independent body and the establishment of adequate oversight mechanisms. Cross-border requests may also negatively impact individuals' access to appeals and remedial mechanisms. Particularly concerning is the possibility that States with weak rule of law and/or problematic human rights records could obtain access to sensitive information about individuals without adequate protections against human rights abuses.

IV. Responsibilities of States

A. State responsibility to respect and duty to protect the right to privacy in the digital age

23. Article 2 (1) of the International Covenant on Civil and Political Rights requires States to "respect and ensure" the rights recognized in the Covenant for all individuals within their territory and subject to their jurisdiction, without discrimination. States parties must refrain from violating the rights recognized in the Covenant, and any restrictions on any of those rights must be permissible under the relevant provisions of the Covenant.[30]

Amnesty International, "Encryption. A matter of human rights" (March 2016); and Wolfgang Schulz and Joris van Hoboken, "Human rights and encryption", United Nations Educational, Scientific and Cultural Organization (2016).

[27] See www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138.

[28] See Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing between Governments and the Need for Safeguards* (April 2018) and www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf.

[29] See submission of Privacy International.

[30] See Human Rights Committee, general comment No. 31, para. 6.

However, the obligations of States extend beyond the obligation to respect and also include "positive" measures to protect the enjoyment of rights. In the context of the right to privacy, that implies a duty to adopt legislative and other measures to give effect to the prohibition of and protection against unlawful or arbitrary interference and attacks, whether they emanate from State authorities or from natural or legal persons.[31]

24. The duty to protect is reflected in pillar I of the Guiding Principles on Business and Human Rights, entitled the "State duty to protect human rights", which elaborates on the implications of the duty of States to protect against adverse human rights impacts involving companies. Principle 1 of the Guiding Principles requires that appropriate steps be taken to prevent, investigate, punish and redress human rights abuses through effective policies, legislation, regulations and adjudication. The subsequent principles outline the different legal and policy areas in which States should adopt a "smart mix of measures" — national and international, mandatory and voluntary — to foster business respect for human rights.[32] Examples of the application of the approach stipulated in the Guiding Principles in relation to the ICT sector include sectoral guidance developed at the European Union level, which focuses on how ICT enterprises should deal with any detrimental impact of their activities.

25. The duty of States to protect against abuses of the right to privacy by companies and other third parties incorporated or domiciled within their jurisdiction has extraterritorial effects. For example, States should have in place export control regimes applicable to surveillance technology, which provide for assessing the legal framework governing the use of the technology in the destination country, the human rights record of the proposed end user and the safeguards and oversight procedures in place for the use of surveillance powers. Human rights guarantees need to be included in export licensing agreements. Furthermore, States have a duty to protect persons within their jurisdictions from extraterritorial interference with their rights to privacy, such as means of interception of communications or hacking.

B. State responsibility to put in place adequate safeguards and effective oversight

26. Enjoyment of the right to privacy depends largely on a legal, regulatory and institutional framework that provides for adequate safeguards, including effective oversight mechanisms. In an era where a vast amount of personal data is accessible to States and business enterprises, and individuals have limited insight into and control over how information about them and their lives is being used, it is critical to focus on measures that mitigate the impact on human rights from such power and information asymmetries.

1. Overarching framework protecting against undue interference

27. One cornerstone of a State privacy protection framework should be laws setting the standards for the processing of personal information by both States and private actors.[33] While States have discretion in defining the smart mix of measures governing the corporate use of personal information, article 17 (2) of the International Covenant on Civil and Political Rights lays down the need to protect individuals by means of law. The increased interlinking of public and private data processing and the track record to date implying mass, recurrent misuse of personal information by some business enterprises confirm that legislative measures are necessary for achieving an adequate level of privacy protection.[34]

---

[31] See Human Rights Committee, general comments No. 16, paras. 1 and 9, and No. 31, para. 8.

[32] See Principle 2, commentary.

[33] See Human Rights Committee, general comment No. 16, para. 9, A/HRC/13/37, para. 61, and A/HRC/17/27, para. 56. For a global overview of data privacy legislation, see Graham Greenleaf, University of New South Wales, submission for the present report. In the present report "processing" is understood as encompassing any operation performed on personal data, including collection, retention, use, modification, erasure, disclosure, transfer and combination.

[34] See Human Rights Council resolutions 34/7, para. 5 (f), and 38/7, para. 17.

28. There is a growing global consensus on minimum standards that should govern the processing of personal data by States, business enterprises and other private actors. International instruments and guidelines reflecting this development include the 1990 Guidelines for the Regulation of Computerized Personal Data Files; the Council of Europe 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its modernized version, which sets a global high level of protection;[35] the 1980 Organization for Economic Cooperation and Development Privacy Guidelines, updated in 2013; the 2014 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention); the Madrid resolution of the International Conference of Data Protection and Privacy Commissioners; and the 2015 Asia-Pacific Economic Coordination Privacy Framework, among others. Those standards, particularly the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, have informed the data privacy frameworks of many States and can direct the design of adequate policy instruments.[36]

29. The instruments and guidelines mentioned above contain a range of key principles, rights and obligations that ensure a minimum level of protection of personal data. First, processing of personal data should be fair, lawful and transparent. The individuals whose personal data are being processed should be informed about the data processing, its circumstances, character and scope, including through transparent data privacy policies. In order to prevent the arbitrary use of personal information, the processing of personal data should be based on the free, specific, informed and unambiguous consent of the individuals concerned, or another legitimate basis laid down in law.[37] Personal data processing should be necessary and proportionate to a legitimate purpose that should be specified by the processing entity. Consequently, the amount and type of data and the retention period need to be limited, data must be accurate and anonymization and pseudonymization techniques used whenever possible. Changes of purpose without the consent of the person concerned should be avoided and when undertaken, should be limited to purposes compatible with the initially specified purpose. Considering the vulnerability of personal data to unauthorized disclosure, modification or deletion, it is essential that adequate security measures be taken. Moreover, entities processing personal data should be accountable for their compliance with the applicable data processing legal and policy framework. Finally, sensitive data should enjoy a particularly high level of protection.[38]

30. In all the instruments and guidelines mentioned above, it is recognized that certain rights need to be afforded to the persons whose data is being processed. At a minimum, the persons affected have a right to know that personal data has been retained and processed, to have access to the data stored, to rectify data that is inaccurate or outdated and to delete or rectify data unlawfully or unnecessarily stored. Newer instruments have added important additional rights, in particular, a right to object to personal data processing, at least for cases where the processing entity does not demonstrate legitimate, overriding grounds for the processing.[39] States should pay particular attention to providing strong protection against interference with the right to privacy by means of profiling and automated decision-making. The rights described above should also apply to information derived, inferred and predicted by automated means, to the extent that the information qualifies as personal data. It is important that the legal framework ensures that those rights do not unduly limit the

[35] In addition to the 47 member States of the Council of Europe, the Convention has been ratified by Mauritius, Senegal, Tunisia and Uruguay, and several other States are in the process of accession.

[36] For detailed guidance, see https://privacyinternational.org/advocacy-briefing/2165/guide-policy-engagement-data-protection and Access Now, "Creating a data protection framework: a do's and don'ts guide for lawmakers. Lessons from the EU general data protection regulation" (2018).

[37] See article 5 (2) of the modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; article 13 (1) of the Malabo Convention; and principle 12 of the Madrid resolution.

[38] See article 6 of the modernized Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

[39] Ibid., art. 9 (1) (d). See also article 21 of the general data protection regulation and article 18 (1) of the Malabo Convention.

right to freedom of expression, including processing of personal data for journalistic, artistic and academic purposes.

31. Data privacy frameworks should also establish certain obligations of the entities processing personal data. Those requirements encompass organizational aspects, such as the establishment of an internal supervisory mechanism, but also include mandatory actions, such as data breach notifications and privacy impact assessments. In an increasingly complex technological environment, such assessments assume a key role in preventing and mitigating privacy harms.[40] Moreover, requirements related to the design of products and services, such as privacy by design[41] and privacy by default,[42] are essential tools for safeguarding the right to privacy.

32. In a globalized world, transfers of data, including large amounts of personal data are commonplace and necessary for the operation of many services. States must ensure that such transfers do not amount to or facilitate undue interference with the right to privacy. At the same time, strict data localization requirements that oblige all data processing entities to store all personal data within the country at issue should be avoided (see A/HRC/32/38, para. 61). Instead, States should focus on ways to ensure that personal data transferred to another State is protected at least at the level required by international human rights law.

33. States should establish independent oversight bodies for the processing of personal data. Such bodies are essential for safeguarding the human rights of the individual against excessive practices of personal data processing. A supervisory authority requires a statutory footing in order to establish clearly its mandate, powers and independence. Such oversight bodies should be provided with the technical, financial and human resources necessary for effective monitoring of the data-processing activities of States and business enterprises, and for enforcing legal requirements in that regard. Moreover, such bodies need to have sufficient legal authority to carry out their functions, including imposing sanctions proportionate to the violations or abuses committed.[43]

2. Procedural safeguards and oversight for surveillance and communications interception

Safeguards

34. While all types of State surveillance-related activities must be conducted on the basis of a law (see A/HRC/27/37, para. 28), the Special Rapporteur on the right to privacy has called attention to the widespread absence of such legislation. It is noteworthy that in many jurisdictions, intelligence and law enforcement agencies are excluded from the provisions of data privacy legislation. Such exceptions should be limited, based on the principles of necessity and proportionality, in order to ensure an adequate level of data privacy in all branches of government. Surveillance-specific legislation should be guided by the following minimum standards.

35. The law must be publicly accessible. Secret rules and secret interpretations of law do not have the necessary qualities of "law" (ibid., para. 29). Laws need to be sufficiently precise. Discretion granted to the executive or a judge and how such discretion may be exercised must be circumscribed with reasonable clarity (see A/69/397, para. 35).[44] To that end, the nature of the offence and the category of persons that may be subjected to surveillance must be described. Vague and overbroad justifications, such as unspecific references to "national security" do not qualify as adequately clear laws. Surveillance must be based on reasonable suspicion and any decision authorizing such surveillance must be

[40] For an in-depth analysis of approaches to privacy impact assessments, see David Wright and Paul de Hert, eds., *Privacy Impact Assessment* (New York, Springer, 2012).

[41] Meaning that privacy protection must be integrated from the outset when designing a system.

[42] Requiring that a system applies privacy-respecting settings by default.

[43] See, for example, https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

[44] See also *Roman Zakharov v. Russia*, para. 230.

sufficiently targeted.[45] The law must strictly assign the competences to conduct surveillance and access the product of surveillance to specified authorities.

36. In terms of its scope, the legal framework for surveillance should cover State requests to business enterprises. It should also cover access to information held extraterritorially or information-sharing with other States. A structure to ensure accountability and transparency within governmental organizations carrying out surveillance needs to be clearly established in the law.

37. Powers of secret surveillance can only be justified as far as they are strictly necessary for achieving a legitimate aim and meet the proportionality requirement (see A/HRC/23/40, para. 83 (b)).[46] Secret surveillance measures must be limited to preventing or investigating the most serious crimes or threats. The duration of the surveillance should be limited to the strict minimum necessary for achieving the specified goal. There must be rigorous rules for using and storing the data obtained and the circumstances in which the data collected and stored must be erased need to be clearly defined, based on strict necessity and proportionality.[47] Intelligence-sharing must be subject to the same principles of legality, strict necessity and proportionality.

38. Where Governments consider targeted hacking measures, they should take an extremely cautious approach, resorting to such measures only in exceptional circumstances for the investigation or prevention of the most serious crimes or threats and with the involvement of the judiciary (see CCPR/C/ITA/CO/6, para. 37).[48] Hacking operations should be narrowly designed, limiting access to information to specific targets and types of information. States should refrain from compelling private entities to assist in hacking operations, thereby impacting the security of their own products and services. Compelled decryption may only be permissible on a targeted, case-by-case basis and subject to judicial warrant and the protection of due process rights (see A/HRC/29/32, para. 60).

Independent authorization and oversight[49]

39. Surveillance measures, including communications data requests to business enterprises and intelligence-sharing, should be authorized, reviewed and supervised by independent bodies at all stages, including when they are first ordered, while they are being carried out and after they have been terminated (see CCPR/C/FRA/CO/5, para. 5).[50] The independent body authorizing particular surveillance measures, preferably a judicial authority, needs to make sure that there is clear evidence of a sufficient threat and that the surveillance proposed is targeted, strictly necessary and proportionate and authorize (or reject) ex ante the surveillance measures.

40. Oversight frameworks may integrate a combination of administrative, judicial and/or parliamentary oversight.[51] Oversight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources. Authorization and oversight should be institutionally separated. Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and have access to the products of surveillance, and carry out periodic reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the oversight bodies,

[45] Ibid., paras. 248 and 260.

[46] See also *Szabo and Vissy v. Hungary*, para. 73.

[47] See *Roman Zakharov v. Russia*, para. 231.

[48] See also Access Now, "A human rights response to government hacking" (September 2016) and Privacy International, "Government hacking and surveillance: 10 necessary safeguards".

[49] See A/HRC/34/60 and European Agency for Fundamental Rights, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update*, (Luxembourg, Publications Office of the European Union, 2017).

[50] See also *Roman Zakharov v. Russia*, para. 233.

[51] See General Assembly resolution 71/199, para. 5 (d).

and they should be required to keep records of all surveillance measures taken.[52] Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review. Exposing oversight bodies to divergent points of view, for example through expert and multi-stakeholder consultations (see for example A/HRC/34/60, para. 36), is particularly important in the absence of an adversarial process: it is essential that "points of friction" — continual challenges to approaches and understandings — be built in.[53]

Principle of transparency

41. State authorities and oversight bodies should also engage in public information about the existing laws, policies and practices in surveillance and communications interception and other forms of processing of personal data, open debate and scrutiny being essential to understanding the advantages and limitations of surveillance techniques (see A/HRC/13/37, para. 55). Those who have been the subject of surveillance should be notified and have explained to them ex post facto the interference with their right to privacy. They also should be entitled to alter and/or delete irrelevant personal information, provided that information is not needed any longer to carry out any current or pending investigation (see A/HRC/34/60, para. 38).

V. Responsibilities of business enterprises

42. Pillar II of the Guiding Principles on Business and Human Rights provides an authoritative blueprint for all enterprises, regardless of their size, sector, operational context, ownership and structure, for preventing and addressing all adverse human rights impacts, including the right to privacy.[54] It outlines the responsibility of business enterprises to respect all internationally recognized human rights, meaning that they should avoid infringing on the human rights of others and address adverse human rights impacts with which they are involved.[55] The responsibility to respect applies throughout a company's activities and business relationships. It is of particular relevance in the digital space that the responsibility to respect applies, regardless of where the people affected are located. The responsibility to respect exists independently of whether the State meets its own human rights obligations.

43. Meeting the responsibility to respect human rights requires that business enterprises (a) avoid causing adverse impacts through their own activities; (b) avoid contributing to adverse impacts through their own activities, either directly or through some outside entity (Government, business or others); and (c) seek to prevent or mitigate adverse human rights impacts directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.[56] For example, a company that provides data about users to a Government that then uses the data to trace and prosecute political dissidents will have contributed to such human rights abuses, including of the right to privacy. Companies that manufacture and sell technologies used for unlawful or arbitrary intrusions will also be contributing to adverse human rights impacts.

44. If there are conflicting demands between respect for international human rights law and obligations under national law, companies should strive to respect international human

[52] See European Court of Human Rights, *Kennedy v. United Kingdom*, application No. 26839/05, judgment of 18 May 2010, para. 165, and *Roman Zakharov v. Russia*, para. 272.

[53] See Human Rights, Big Data and Technology Project, Human Rights Centre, University of Essex, submission for the present report.

[54] The Guiding Principles were unanimously endorsed by the Human Rights Council in its resolution 17/4.

[55] Guiding Principle 11.

[56] Guiding Principle 13. See also OHCHR, "The corporate responsibility to respect human rights: an interpretive guide" (2012).

rights law to the greatest extent possible and mitigate as much as possible any adverse impact, for example by interpreting government demands as narrowly as possible.[57]

45. The responsibility to respect human rights requires business enterprises to have in place policies and processes appropriate to their size and circumstances, including:

(a) Making a publicly available policy commitment at the most senior level and embedding responsibility to respect human rights throughout operational policies and procedures;[58]

(b) Carrying out human rights due diligence processes, which entails:

(i) Conducting human rights impact assessments to identify and assess any actual or potentially adverse human rights impacts;

(ii) Integrating those assessments and taking appropriate action to prevent and mitigate adverse human rights impacts that have been identified;

(iii) Tracking the effectiveness of their efforts;

(iv) Reporting formally on how they have addressed their human rights impacts;[59]

(c) Providing remediation or cooperating in remediation of abuse where the company identifies adverse impacts that it has caused or to which it has contributed.[60]

46. According to the Guiding Principles, all companies have a responsibility to undertake human rights due diligence to identify and address any human rights impacts of their activities. Taking a concrete example, companies selling surveillance technology should carry out, as part of their due diligence, a thorough human rights impact assessment prior to any potential transaction. Risk mitigation should include clear end-use assurances being stipulated in contractual agreements with strong human rights safeguards that prevent arbitrary or unlawful use of the technology and periodic reviews of the use of technology by States.[61] Companies collecting and retaining user data need to assess the privacy risks connected to potential State requests for such data, including the legal and institutional environment of the States concerned. They must provide for adequate processes and safeguards to prevent and mitigate potential privacy and other human rights harms. Human rights impact assessments also need to be conducted, as part of the adoption of the terms of service and design and engineering choices that have implications for security and privacy, and decisions taken to provide or terminate services in a particular context (see A/HRC/32/38, para. 11).

47. As part of the human rights due diligence process, the Guiding Principles stipulate that business enterprises should account for how they address their human rights impacts and be prepared to communicate that externally, particularly when concerns are raised by or on behalf of affected stakeholders.[62] In the digital environment, that entails disclosing which personal data are collected, how long they are stored for, for what purpose, how they are used and with whom and under what circumstances they are shared. That includes requests received by States for access to user data. In instances where national laws and regulations hinder such reporting, companies should use to the greatest extent possible any leverage they may have and are encouraged to advocate for the possibility to release such information.

48. As part of the operationalization of their policy commitments under the Guiding Principles, the ICT sector has developed guidance on how to implement human rights policies. Such initiatives include the Principles on Freedom of Expression and Privacy of

[57] Guiding Principle 23.
[58] Guiding Principle 16.
[59] Guiding Principles 17–21.
[60] Guiding Principle 22 and section VI of the present report.
[61] See Privacy International, submission to the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (January 2016), available at www.ohchr.org/Documents/Issues/Expression/PrivateSector/PrivacyInternational.pdf.
[62] Guiding Principle 21.

the Global Network Initiative (the GNI Principles)[63] and the Telecommunications Industry Dialogue Guiding Principles.[64] For example, the GNI principles specifically state that participating companies "will employ protections with respect to personal information" and "will respect and work to protect the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards".

49. The Ranking Digital Rights Corporate Accountability Index evaluates a number of Internet, mobile and telecommunications companies specifically on their disclosed commitments and policies affecting freedom of expression and privacy.[65] That can be a useful tool for holding companies accountable for their impact on users' rights.

VI. Remedies

50. Victims of privacy violations or abuses committed by States and/or business enterprises must have access to an effective remedy. States not only have obligations to ensure accountability and remedy for human rights violations committed by State actors, they must also take appropriate steps to ensure that victims of business-related human rights abuse have access to an effective remedy (see pillar III of the Guiding Principles on Business and Human Rights). Depending on the nature of a particular case or situation, victims should be able to achieve remedies through effective judicial or non-judicial State-based grievance mechanisms (A/HRC/32/19, Corr. 1 and Add. 1 and A/HRC/38/20 and Add. 1). Relevant State-based non-judicial mechanisms in the ICT context include independent authorities with powers to monitor State and private sector data privacy practices, such as privacy and data protection bodies.

51. Under the Guiding Principles, where business enterprises determine that they have caused or contributed to adverse human rights impacts, they should provide for or cooperate in the remediation of any adverse human rights impacts that they may have caused or contributed to through legitimate processes.[66] For any non-judicial mechanism to be effective, it should be legitimate, accessible, predictable, equitable, rights-compatible, transparent, a source of continuous learning and, for operational level grievance mechanisms, based on dialogue and engagement.[67]

52. Where an enterprise has not caused or contributed to an adverse impact, but where the impact is directly linked to its operations, products or services by a business relationship, the appropriate action is elaborated in Guiding Principle 19. It may include using any leverage the enterprise may have over its business partner or client to seek to influence it to provide for remediation.[68]

53. The Guiding Principles also highlight the role that operational-level grievance mechanisms can have in addressing grievances directly. Such mechanisms can potentially take a range of forms, which will depend on the type of company concerned, the needs of its stakeholders and the company's human rights risk picture. To identify how those mechanisms may be designed and work in the ICT sector in practice, further discussion within the sector and with stakeholders is necessary.

54. In practice, there are significant gaps and obstacles when it comes to providing access to remedial avenues for privacy infringements. The transnational nature and effects of surveillance, communications interceptions and the many forms of processing of personal data pose legal and practical challenges (see A/HRC/34/60, para. 34). In addition,

[63] Available from https://globalnetworkinitiative.org/gni-principles/. See also the Global Network Initiative, submission for the present report.

[64] Available from www.telecomindustrydialogue.org/about/guiding-principles/.

[65] See https://rankingdigitalrights.org/index2018/.

[66] Guiding Principle 22.

[67] Guiding Principle 31.

[68] Guiding Principle 19 and its commentary. See also OHCHR, "The corporate responsibility to respect human rights: an interpretive guide", pp. 48–52.

victims' lack of knowledge or proof of undue interference is a frequent obstacle to access to remedies (see A/HRC/27/37, para. 40). For example, State requests to access data held by companies are often accompanied by "gag orders" prohibiting companies from notifying the individuals concerned. States also often fail to notify those affected by other surveillance measures, in particular in mass surveillance cases. Recognizing that advance or concurrent notification might jeopardize the effectiveness of legitimate surveillance measures, individuals should nevertheless be notified once surveillance has been completed (see A/HRC/23/40, para. 82). If that is not possible, the law should generously grant standing to those who may theoretically have been affected by those measures (see A/HRC/13/37, para. 38). Similarly, business enterprises should notify their customers once they become aware of personal data breaches that may have affected their rights.

55. Victims also face new and growing challenges in the context of algorithmic decision-making, where individuals may not be able to access the input data or challenge the findings reached by the algorithm itself or how such findings were used in the decision reached.[69] States and business enterprises, in collaboration with other stakeholders, should consider possible mechanisms for addressing this issue, such as the creation of well-resourced expert auditing bodies.

56. The nature of the harm caused by privacy infringements is the source of further challenges. The effect of privacy breaches is difficult to undo and may result in ongoing consequences and further human rights implications. The ease of retaining, sharing, repurposing and fusing data and profiles influences the permanence of digital data, meaning an individual may face new and ongoing risks to their rights into the future.[70]

57. Privacy harms significantly affect a person's life, even when there is no quantifiable economic or other impact; the nature of the harm should not prevent victims from seeking redress. For instance, consumer protection organizations could be empowered to seek redress on behalf of victims of corporate privacy abuses.

VII. Conclusions and recommendations

58. The international human right framework provides a strong basis for shaping the responses to the manifold challenges arising in the digital age. There is an urgent need for States to fully implement their obligations to respect the right to privacy, as well as their duty to protect the right to privacy, including vis-à-vis corporate abuses. To accomplish that objective, States need to establish an appropriate legal and policy framework, including adequate privacy protection legislation and regulation that incorporate the principles of legality, proportionality and necessity, and establish safeguards, oversight and remedies.

59. Many issues that could not be addressed in the present report require further in-depth study, including the interrelationships of the right to privacy with other human rights, including economic, social and cultural rights; disproportionate or discriminatory impacts of privacy invasions on individuals and/or groups at risk; the effects of big data and machine learning, including for predictive and pre-emptive purposes, on the enjoyment of the right to privacy and other human rights; and the regulation of surveillance technology markets.

60. The nature and forms of remedies that respond effectively to situations where the right to privacy has been violated is another area in which further attention is warranted. As a first step, the types of remedial action that would be appropriate in different situations should be identified in a systematic way. That could be used in the development of further guidance. In undertaking that analysis, due regard should be paid to the guidance and recommendations developed through the accountability and remedy project of the Office of the United Nations High Commissioner for Human

[69] See submission of the University of Essex Human Rights, Big Data and Technology Project, para. 33.
[70] Ibid, para. 7.

Rights (OHCHR). More generally, efforts should be made to develop sector-specific guidance tools on business responsibilities to respect the right to privacy.

61. The High Commissioner recommends that States:

(a) Recognize the full implications of new technologies, in particular data-driven technologies for the right to privacy but also for all other human rights;

(b) Adopt strong, robust and comprehensive privacy legislation, including on data privacy, that complies with international human rights law in terms of safeguards, oversight and remedies to effectively protect the right to privacy;

(c) Ensure that data-intensive systems, including those involving the collection and retention of biometric data, are only deployed when States can demonstrate that they are necessary and proportionate to achieve a legitimate aim;

(d) Establish independent authorities with powers to monitor State and private sector data privacy practices, investigate abuses, receive complaints from individuals and organizations, and issue fines and other effective penalties for the unlawful processing of personal data by private and public bodies;

(e) Ensure, through appropriate legislation and other means that any interference with the right to privacy, including by communications surveillance and intelligence-sharing, complies with international human rights law, including the principles of legality, legitimate aim, necessity and proportionality, regardless of the nationality or location of the individuals affected, and clarify that authorization of surveillance measures requires reasonable suspicion that a particular individual has committed or is committing a criminal offence or is engaged in acts amounting to a specific threat to national security;

(f) Strengthen mechanisms for the independent authorization and oversight of State surveillance and ensure that those mechanisms are competent and adequately resourced to monitor and enforce the legality, necessity and proportionality of surveillance measures;

(g) Review laws to ensure that they do not impose requirements of blanket, indiscriminate retention of communications data on telecommunications and other companies;

(h) Take steps in order to enhance transparency and accountability in the acquisition of surveillance technologies by States;

(i) Fully implement their duty to protect against abuses of the right to privacy by business enterprises in all relevant sectors, including the ICT sector, by taking appropriate steps to prevent, investigate, punish and redress such abuse through effective policies, legislation, regulations and adjudication;

(j) Ensure that all victims of violations and abuses of the right to privacy have access to effective remedies, including in cross-border cases.

62. The High Commissioner recommends that business enterprises:

(a) Make all efforts to meet their responsibility to respect the right to privacy and all other human rights. At a minimum, business enterprises should fully operationalize the Guiding Principles on Business and Human Rights, which implies conducting effective human rights due diligence across their operations and in relation to all human rights, including the right to privacy, and taking appropriate action to prevent, mitigate and address actual and potential impacts;

(b) Seek to ensure a high level of security and confidentiality of any communications they transmit and personal data they collect, store or otherwise process. Conduct assessments on how best to design and update the security of products and services on an ongoing basis;

(c) Comply with the key privacy principles referred to in paragraphs 29–31 of the present report and ensure the greatest possible transparency in their internal policies and practices that implicate the right to privacy of their users and customers;

(d) Provide for or cooperate in remediation through legitimate processes where they have caused or contributed to adverse impacts, including through effective operational-level grievance mechanisms;

(e) Contribute to the work of the OHCHR accountability and remedy project on developing guidance and recommendations to enhance the effectiveness of non-State-based grievance mechanisms in relation to abuses of the right to privacy in the digital space.